International Journal of Computer Science and Information Technology
ISSN: 3005-9682 (Print), ISSN: 3005-7140 (Online) | Volume 3, Number 3, Year 2024
DOI: https://doi.org/10.62051/ijcsit.v3n3.38
Journal homepage: https://wepub.org/index.php/IJCSIT/index

Physical Damage to the Circuit Overview Based on FPGA

Hua Wang

College of Electronic Information, Xinan Minzu University, Chengdu, China

ABSTRACT

At present, the main hardware vulnerabilities of FPGA come from the security threats of hardware backdoors. A hardware backdoor is a malicious circuit planted in an FPGA that, if activated, will cause the FPGA to perform unintended functions. The hardware backdoor is composed of trigger and payload. When the condition of the trigger is satisfied, the malicious function will be realized through the payload circuit. Hardware backdoors often result in data errors, functional failures, information leaks, unauthorized access, and even shortened lifetime of FPGAs.

KEYWORDS

FPGA; Hardware Security; Hardware Backdoor

1. INTRODUCTION

In recent years, there is a new kind of attack circuit, that is, physical damage circuit, which will make the dynamic current of FPGA increase sharply after being activated. On the one hand, the surge current will cause the voltage fluctuation of the FPGA power supply pin, so that the timing constraints of some critical paths can no longer be satisfied, leading to the functional failure of the FPGA. On the other hand, the increase in FPGA power consumption over a long period of time will make the device heat significantly, which will induce the device to enter a state of overheating, and even cause the device to burn. According to our research experience, FPGA physical damage circuits are divided into two types: short circuit attack and voltage drop attack. The current typical physical damage circuits and their detection methods are summarized in Table 1.

In terms of short-circuit attack and detection: As early as 1999, Hadzic et al from the University of Pennsylvania in the United States demonstrated a special FPGA attack mode, which would send multiple driver modules inside the FPGA to the same wired resource and thus generate a short circuit [18]. Hadzic et al. demonstrated the effectiveness of this attack method on Altera's Flex8000 series FPGAs. Although this attack exploits the specific structure of the shared column connection in the Flex8000FPGA, most modern FPGAs do not allow multiple devices to drive the same connection, and this short-circuit connection configuration is easily detected by bitstream detection tools, this method is the first to demonstrate the feasibility of a short-circuit attack.

In 2010, Beckhoff et al. from the University of Oslo in Norway proposed the first practical FPGA short-circuit attack circuit, which overwrites the configuration bit of the internal multiplexer of CLB (ConfigurableLogicBlock, programmable logic block) through the run-time reconfiguration function of FPGA. Various short-circuit attack circuits, such as short, medium and long term, have been realized [17]. In XilinxVirtex-IIFPGA, a single attack circuit can increase current consumption by more than 12.7mA. Beckhoff noted that the short-circuit attack circuit cannot be detected in the synthesis phase, but can be identified by the ReCoBus bitstream detection tool.

Table 1. FPGA physical damage circuit and detection methods

Attack type	Damage circuit	Detection method
Short-circuit attack	Multiple device drivers share column connections. University of Pennsylvania, 1999, Hadvic [16]	Bitstream Check
	Multiplexer and runtime reconfiguration. University of Oslo, Norway, 2010, Beckhoff [17]	ReCoBus
	PS-DAC, Change the PIP configuration bit. 2014, Brigham Young University, Daniel [18]	Bitstream Check
Power drop attack	LUT5-RO, FPGAhammer. 2017-2018, University of Karlsruhe, Germany, Gnad et al [21]	Bitstream Check*
	LUT6-RO, MUX-RO, FF-RO, etc. 2019, University of Manchester, UK, La et al [23]	FPGADefender*
	D Latch -RO, Burr clock oscillator. 2019, University of Karlsruhe, Germany, Krautter et al [22]	null
	GlitchAmplification. 2020, University of Manchester, UK, Matas et al [25]	null
	* This detection method has limitations	

In terms of power drop attacks and detection: In 2011, Ziener et al. from the Software/Hardware Collaborative Laboratory of University of Erlangen-Nuremberg in Germany proposed a novel FPGA module design [19], which connects multiple cycle shift registers to the same clock signal and changes the data flip rate by enabling/disabling shift registers, thus affecting the power consumption of FPGA. To artificially introduce a voltage drop on the FPGA power supply pin. While the module is designed to divulge internal information through voltage changes in the power pin (i.e., the FPGA power side channel), the module clearly demonstrates for the first time how operating data flip rates can affect FPGA power, triggering a device voltage drop. Then in 2013, Zick et al., from the Information Science Research Center of the University of Southern California, used Torc software tool to connect a large number of unused PIPs in XilinxKIntex-7 FPGA to the same signal, and flipped the levels on these signal wires to increase the device power instantaneously. Can result in a 31% instantaneous voltage drop on the FPGA power supply pin [20]. The above two studies have completed the exploration of the principle of voltage drop attack, paving the way for the practical design of FPGA voltage drop attack.

Based on the above theoretical exploration of voltage drop attack, the first FPGA voltage drop attack circuit was the LUT5-RO circuit proposed by Gnad et al of the Computing Science Research Center of the University of Karlsruhe in Germany in 2017 [21]. Gnad et al. looped the output port of the LUT5 unit configured as a reverse gate in the FPGA to the input port, thus forming a RO (RingOscillator, ring oscillator) circuit, and connected multiple RO to the same enable signal for control, through the rapid self-oscillation of the RO circuit to implement voltage drop attack. Experiments show that the voltage drop attack circuit can be generated by standard FPGA design tools and can successfully crash XilinxVirtex6, Kintex7, Zynq7000 and other types of FPGA systems. It should also be noted that Gnad notes that only some of the latest FPGA design software has a BitstreamCheck feature that allows combinatorial logic checks to prevent combinatorial logic loopback circuits like RO, and that this feature can be intentionally turned off. Therefore, innovative efforts are needed to effectively detect and prevent such attacks.

The attack method of Gnad et al. has been improved in literature [25]. In 2018, his team's Krautter et al. showed that by making RO self-oscillate at a slower frequency and continuously enable/disable individual RO in the RO array, a more significant attack effect can be produced. The proposed FPGAHammer attack method still uses LUT5-RO circuit, but a special RO activation mode is designed to maximize the effect of voltage drop attack.

In 2019, La et al., University of Manchester, UK, conducted a detailed study on RO-based voltage drop attack circuits in literature [23], and expanded a variety of deformation circuits such as LUT6-RO, MUX7-RO, MUX8-RO and FF-RO on the basis of Gnad research. Meanwhile, aiming at RO-based voltage drop attack circuit, La et al. proposed a defense tool FPGADefend, which can detect and identify self-oscillating circuit in FPGA to prevent RO voltage drop attack. FPGADefend can successfully prevent basic RO attacks, but with the development of attack means, new defense means need further research.

In 2019, Krautter et al. further improved the RO circuit in literature [24] and proposed two non-combinational logic voltage drop attack circuits: D-latch-RO circuit and burr clock-based oscillator circuit [28]. Since these two attack circuits are composed of sequential logic, BitstreamCheck's combinatorial logic check function is disabled against them.

In 2020, Matas et al. from La's team proposed the voltage drop attack circuit for GlitchAmplification, which consists of two parts: the burr generating circuit and the power consumption network [25]. The burr generating circuit consists of an XOR gate with a multistage delay input (XOR tree), which can produce a rapidly flipping burr signal at the XOR gate output by carefully adjusting the delay length. The power consumption network is composed of wired resources all over the FPGA. When the burr signal is transmitted on the network, it can consume a lot of FPGA power consumption and cause voltage drop. Matas points out that because the GlitchAmplification circuit does not contain an RO oscillator, this cannot be detected by detection tools such as FPGADefender.

2. MECHANISM OF FPGA DAMGE CIRCUIT

2.1. Formation Mechanism of Short Circuit Attack Circuit

The short-circuit attack circuit causes a short circuit in the circuit by modifying the internal connection configuration of the FPGA, and thus consumes a large amount of power. Depending on the duration of the short circuit, the attack mode can be divided into the following three types:

(1) Long-term short circuit: The short-circuit connection formed can persist for a long time, usually caused by single particle flipping or configuration bit damage.

(2) metaphase short circuit: If a new bit is written without the original configuration bit being cleared during connection configuration data modification, a short circuit may occur a period of time before the new configuration bit is refreshed.

(3) short-term circuit: refers to the short circuit connection whose current peak duration is shorter than 1ns. The generation mechanism of these three short-circuit attacks will be discussed separately below.

2.1.1 Long-term Short Circuit

When configuring a switch matrix multiplexer, there are two possible reasons for a short circuit: 1) there are two or more bits of 1 in the gc; 2) At least one bit is 1 in gc and at least two bits are 1 in gr. If these conditions are met, the inputs of both multiplexers are connected to the outputs at the same time. When the two input drivers are the same logical value, no short circuit will occur; When two input drivers have different logic values, a short circuit occurs.

Assume that the probability that the input drives logic 1 is p, and the probability that the logic 0 is 1-p, and assume that the different input drive values are statistically independent. When the k bit is 1 in g_c and the l bit is 1 in gr, the k×l inputs of the multiplexer will be connected to the output. If all the connected inputs drive the same value, no short circuit will occur. The non-short circuit probability value p_{nsc}, which includes both all inputs of 1 and all inputs of 0, can be expressed by the following formula:

$$p_{nsc} = p^{k-l} + (1 - p)^{k-l} \quad (1)$$

When k=l=1 and only one input and output are connected, then p_{nsc} is equal to 1. In addition, the probability of a short circuit occurring $p_{sc}=1-p_{nsc}$. Because such short-circuit connections can persist during operation, they are classified as long-term short-circuits.

2.1.2 Metaphase Short Circuit

When modifying the connection configuration data, if new bits are written without clearing the original configuration bits, an intermediate short circuit may occur.

Assume that only 1bit of configuration has changed in g_c, and all bits in gr remain unchanged. Let the m_j bit in c1 be 1 and the mi bit in c2 be 1; Assume that the configuration bit mi is on frame f and m_j is on frame g, and that the configuration data of frame f is written before the data of frame g. When the original configuration c1 is still active, the configuration input for frame f of configuration c2 is written, resulting in two bits of 1 in the group g_c. This may cause a short circuit to occur. This short-circuited connection will continue until the c2 configuration has written to frame g. It can be seen that the duration of the intermediate short may increase with the number of frames s

2.1.3 Short-term Circuit

In the above example, m_i and m_j are located in different frames (f and g). If both are in the same configuration frame, the modification of the configuration bits will be completed within one clock cycle. An instantaneous short-circuit connection may still occur at this time, but because of its short existence time, usually less than 1ns, such a short-circuit is classified as a short circuit.

2.2. Voltage Drop Attack Circuit Generation Mechanism

The generation mechanism of the voltage drop attack can be described as: by generating a large amount of bit flipping activity within the FPGA for a short time, it pulls a large amount of current and creates a voltage drop on the FPGA power supply pin. When the voltage drop exceeds the device threshold, the FPGA will enter an abnormal state, and even when the turnover activity stops and the voltage drop disappears, the device still cannot return to the normal working state. At the same time, a large amount of current consumption will cause the device to heat up sharply in a short period of time, resulting in the device entering an overheated state, even until the chip burns. According to different ways of pulling current, the realization of voltage drop attack can be divided into voltage drop attack circuit based on large fan-out RO network and voltage drop attack circuit based on burr amplifier line.

2.2.1. Voltage drop attack circuit based on large fan-out RO network

(1) Combined circuit RO

The original RO was a ring oscillator circuit consisting of an odd number of reversers connected end to end. The frequency of RO can be calculated by the propagation delay of the entire combined loop, including the propagation delay tlogic and path delay tnet of logical blocks such as LUT and DSP, as shown in equation (2):

$$f_{RO} = \frac{1}{t_{RO}} = \frac{1}{2 \times (t_{logic} + t_{net})} \quad (2)$$

At present, the existing research uses LUT to realize RO. The project team analyzed the internal architecture of logic (i.e. SliceL/SliceM), arithmetic (i.e. DSP48E2) and BRAM units in UltraScale+FPGA to determine whether they can constitute RO:

Slice: RO can be designed by its internal LUT, D latch, etc. In addition to this, it can also (1) form the path of RO through the on-chip MUX (F7Mux and F8Mux multiplexers); (2) The path of RO is formed by carry logic.

DSP: A counter can be implemented by feeding the output of the DSP back to the input without using any registers in the feedback path to form an RO. The DSP48E2 primitive includes not only a multiplier, but also an ALU that can perform bit operations faster than arithmetic operations.

BRAM: BRAM consists primarily of sequential circuits, where the only combined part is located in its cascading logic. However, cascading chains have dedicated bottom-up routing resources that cannot be controlled by user logic, and cascading multiplexers are controlled by triggers. Therefore, you cannot build RO using BRAM.

In terms of the efficiency of RO voltage drop attacks, even for basic RO using LUT, we find that different LUT6 units within CLB and RO implemented with different LUT inputs vary considerably in oscillation frequency and current consumption. The oscillation frequency of RO is distributed in the range of 1GHz to 6GHz, and the current power is not necessarily related to the flipping frequency of the oscillator. Because the propagation path is longer RO although the oscillation frequency is lower, but because the path is longer, the current consumption of the signal propagation process is higher.

(2) Uncombined circuit RO

Another way to implement RO is to introduce an uncombined circuit loop. For example, by creating multiple paths of different propagation delays from the output of a single T flip-flop to the LUT, this will result in a short flip of the level at the LUT output configured as an XOR gate. The LUT output is then fed back to the clock input pin of the T flip-flop, from which an uncombined circuit RO is created. When the time difference between the two output paths of the T flip-flop is 218ps, the oscillation frequency of the measured RO is 481MHz. You can also manually optimize the RO's oscillation frequency by using different local routing options to fine-tune the routing latency.

2.2.2. Voltage drop attack circuit based on burr amplification

In a timing design, the output of the trigger can change state at most every clock cycle, so its activity factor is 1/2 of the clock frequency. For example, if the output of a trigger is fed back to the input through a reverse gate, the activity factor of the loop is equal to the general clock frequency. However, by implementing the combinatory logic of inputs with different propagation delays into the FPGA, a burr will be created as shown in the figure below.

Increasing the activity factor by a burr amplifier circuit can produce frequent turnover activity that has consumed a large amount of current. The burr amplification attack circuit consists of two parts: burr generating circuit and current consuming circuit. The burr generating circuit is a standard T flip-flop with a delay chain and a wide input XOR gate. For example, the output of a 200MHz T flip-flop is connected to a delay chain and plugged into a 6-input XOR gate. By adjusting the delay value of the delay chain, the activity factor of the XOR gate can be 3. At this point, the output of XOR can reach 3 times the clock frequency (600MHz). The burr amplifier circuit consists of lines throughout the FPGA. In the burr amplification line voltage drop attack circuit, the main source of current consumption is not the burr generating circuit itself, but the wires and components on the current consumption network path. Therefore, the attack circuit has strong concealment.

3. CONCLUSION

It is found that when a certain number of RO rings are deployed and a suitable switching frequency is given to the RO rings, the voltage drop attack will be upgraded to a DoS attack, the FPGA chip will crash.

REFERENCES

[1] Broy M. Engineering cyber-physical systems: Challenges and foundations [M]. Complex Systems Design & Management. Springer, Berlin, Heidelberg, 2013: 1-13.

[2] Congmiao L, Srinivasan D, Reindl T. Malware Detection for Cyber Security Enhancement in Smart Grid [C]. Proceedings on International Conference on Emerg. 2018, 2: 30-36.

[3] Total Microprocessor Sales to Edge Slightly Higher in 2020 [EB/OL]. https://www.icinsights.com/news/bulletins/Total-Microprocessor-Sales-To-Edge-Slightly-Higher-In-2020/

[4] The National Strategy to Secure Cyberspace [EB/OL]. https://georgewbush-whitehouse.archives.gov/pcipb/text/

[5] Haizler O. The United States' cyber warfare history: Implications on modern cyber operational structures and policymaking [J]. Cyber, Intelligence, and Security, 2017, 1(1): 31-45.

[6] Tromparent P. French cyberdefence policy [C]. 2012 4th International Conference on Cyber Conflict (CYCON 2012). IEEE, 2012: 1-12.

[7] Cohen M S, Freilich C D, Siboni G. Israel and cyberspace: Unique threat and response [J]. International Studies Perspectives, 2016, 17(3): 307-321.

[8] Tabansky L. Cyber Power in the changing Middle East [J]. Turkish Policy Quarterly, 2016, 15(1): 107-114.

[9] Chen T M. Stuxnet, the real start of cyber warfare? [Editor's Note] [J]. IEEE Network, 2010, 24(6): 2-3.

[10] Kim A, Wampler B, Goppert J, et al. Cyber attack vulnerabilities analysis for unmanned aerial vehicles [M]. Infotech@ Aerospace 2012. 2012: 2438.

[11] Verble J. The NSA and Edward Snowden: surveillance in the 21st century [J]. Acm Sigcas Computers and Society, 2014, 44(3): 14-20.

[12] Trump Inherits a Secret Cyberwar Against North Korean Missiles [EB/OL]. https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html

[13] Lipp M, Schwarz M, Gruss D, et al. Meltdown: Reading kernel memory from user space [C]. 27th {USENIX} Security Symposium ({USENIX} Security 18). 2018: 973-990.

[14] Kocher P, Horn J, Fogh A, et al. Spectre attacks: Exploiting speculative execution [C]. 2019 IEEE Symposium on Security and Privacy (SP). IEEE, 2019: 1-19.

[15] Giordani A. How Meltdown and Spectre will impact future processor designs: ADRIAN GIORDANI REPORTS ON RECENT VULNERABILITIES FOUND IN MANY MODERN CPUS[J]. Scientific Computing World, 2018 (159): 14-16.

[16] Hadžić I, Udani S, Smith J M. FPGA viruses [C]. International Workshop on Field Programmable Logic and Applications. Springer, Berlin, Heidelberg, 1999: 291-300.

[17] Beckhoff C, Koch D, Torresen J. Short-circuits on FPGAs caused by partial runtime reconfiguration [C]. 2010 International Conference on Field Programmable Logic and Applications. IEEE, 2010: 596-601.

[18] Savory D C. Power side-channel DAC implementations for Xilinx FPGAs [D]. Brigham Young University - Provo, 2014.

[19] Ziener D, Baueregger F, Teich J. Using the power side channel of FPGAs for communication [C]. 2010 18th IEEE Annual International Symposium on Field- Programmable Custom Computing Machines. IEEE, 2010: 237-244.

[20] Zick K M, Srivastav M, Zhang W, et al. Sensing nanosecond-scale voltage attacks and natural transients in FPGAs [C]. Proceedings of the ACM/SIGDA international symposium on Field programmable gate arrays. 2013: 101-104.

[21] Gnad D R E, Oboril F, Tahoori M B. Voltage drop-based fault attacks on FPGAs using valid bitstreams [C]. 2017 27th International Conference on Field Programmable Logic and Applications (FPL). IEEE, 2017: 1-7.

[22] Krautter J, Gnad D R E, Tahoori M B. FPGAhammer: Remote voltage fault attacks on shared FPGAs, suitable for DFA on AES [J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018: 44-68.

[23] La T M, Matas K, Grunchevski N, et al. FPGADefender: Malicious Self-Oscillator Scanning for Xilinx UltraScale+ FPGAs [J]. ACM Transactions on Reconfigurable Technology and Systems (TRETS), 2019, 13(3): 1-31.

[24] Krautter J, Gnad D R E, Tahoori M B. Mitigating electrical-level attacks towards secure multi-tenant FPGAs in the cloud [J]. ACM Transactions on Reconfigurable Technology and Systems (TRETS), 2019, 12(3): 1-26.

[25] Matas K, La T M, Pham K D, et al. Power-hammering through glitch amplification–attacks and mitigation [C]. 2020 IEEE 28th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM). IEEE, 2020: 65-69.

[26] Domas C. Breaking the x86 ISA [J]. Black Hat, USA, 2017.

[27] Dofferhoff R, Göebel M, Rietveld K, et al. iScanU: A Portable Scanner for Undocumented Instructions on RISC Processors [C]. 2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). IEEE, 2020: 306-317.

[28] Strupe F, Kumar R. Uncovering Hidden Instructions in Armv8-A Implementations [C]. Workshop on Hardware and Architectural Support for Security and Privacy. 2020.

[29] Zhu J, Song W, Zhu Z, et al. CPU security benchmark [C]. Proceedings of the 1st Workshop on Security-Oriented Designs of Computer Architectures and Processors. 2018: 8-14.

[30] Li X, Wu Z, Wei Q, et al. Uisfuzz: An efficient fuzzing method for cpu undocumented instruction searching [J]. IEEE Access, 2019, 7: 149224-149236.

[31] Wu J, Cui B, Chen C, et al. A High Efficiency and Accuracy Method for x86 Undocumented Instruction Detection and Classification [C]. International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. Springer, Cham, 2021: 295-303.

[32] X. Wei, Y. Diao and Y. L. Wu. “To Detect, Locate, and Mask Hardware Trojans in digital circuits by reverse engineering and functional ECO”. The 21st Asia and South Pacific Design Automation Conference (ASP-DAC), Macao, 2016: 623-630.

[33] C. Bao, D. Forte and A. Srivastava. “On application of one-class SVM to reverse engineering-based hardware Trojan detection”. The Fifteenth International Symposium on Quality Electronic Design, Santa Clara, 2014: 47-54

[34] R. S. Chakraborty, F. Wolff and S. Paul, et al. “MERO: A statistical approach for hardware Trojan detection”. International Workshop on Cryptographic Hardware and Embedded Systems, Lausanne, 2009: 396-410.